VeriSign®
The Value of Trust℠

Authentication Services

Hardware/Software Requirements

CUSTOMER MANUAL

Customer Support: +44(0) 870 608 7878

support@trustwise.com

BT38-MPKI6-HW-V1.0

Authentication Services Hardware/Software Requirements

BT38-MPKI6-HW-V1.0 has been produced from
VeriSign Inc. Doc Ref 00010846

Copyright © 1998 - 2003 VeriSign, Inc. All rights reserved.
Printed in the United States of America.

Publication date: August 2003
BT Revision date: September 2005

This document supports **Authentication Services 6.0** and all subsequent releases unless otherwise indicated in a new edition or release notes.

U.S. patent 6,324,645

Trademark Notices

VeriSign is a registered trademark of VeriSign, Inc. The VeriSign logo, VeriSign Trust Network, and Go Secure! are trademarks and service marks of VeriSign Inc. XMLPay and OnSite are registered trademarks of VeriSign, Inc. Other trademarks and service marks in this document are the property of their respective owners.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photographic, audio, or otherwise) without prior written permission of VeriSign, Inc. Notwithstanding the above, permission is granted to reproduce and distribute this document on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete form with attribution of the document to VeriSign, Inc

BT Notice

This software and the corresponding documentation are being provided to you in conjunction with the products and services provided to you by BT. The software and documentation was originally designed to be used with products and services offered directly by VeriSign to its customers. BT is offering substantially the same products and services to you as VeriSign provides to its customers. The software and documentation, however, may have been translated and localized by BT. BT assumes all responsibility for the translation and localization of the software and documentation, and VeriSign disclaims any and all warranties, express, implied, or statutory, including without limitation any implied warranty of merchantability or fitness for a particular purpose and refuses liability for such translation and localization.

Note This document may describe features and/or functionality that are not present in your software or your service agreement. Contact your account representative to learn more about what is available with this VeriSign product.

Contents

Chapter 1 Introduction 1

About this Manual 1
Related Managed PKI Documents 3
Compatibility Matrix for Single Digital ID 3

Chapter 2 Managed PKI Requirements 7

Protocols and Ports 7
Internet Access for Authentication Methods 8
Managed PKI Administrator Workstation 9
Hardware 9
Supported Operating Systems 9
Supported Browsers 9
End User Machine 10
Operating System 10
Supported Browsers 10
Local Hosting 10
Supported Web Server Applications 11
Supported Local Hosting Web Server Operating Systems 11
Automated Administration Module 12
Requirements 12
Supported Local Hosting Web Servers 12
Automated Administration Server 13
Automated Administration Data Sources 13
Key Management Service 14
Requirements 14
Key Manager Server 14
Local Hosting Server 15
Key Manager Data Sources 15
Roaming 16
Roaming Service 16
Enterprise Roaming 18
Digital Notarization 21
Web Browser Requirements 21
Certificate Validation Module (CVM) 21
Platforms Supported 22

CVM Web Server Plug-In 22
Certificate Parsing Module (CPM) 23
Online Certificate Status Protocol (OCSP) 24
Browser Requirements 24

Chapter 3 Go Secure! Requirements 25

Go Secure! for Check Point 25
Managed PKI Installation Requirements 25
Browser 25
SecuRemote Version 25
VPN-1 Gateway 26
SecuRemote and SecureClient Workstation 26
Directory Object Module (DOM) Requirements 26
Go Secure! for Lotus Notes 27
Managed PKI Installation Requirements 27
Local Hosting Web Server Operating Systems 27
Web Servers 28
Notes Client Requirements 28
Limitations and Assumptions in Go Secure! for Lotus Notes 28
Go Secure! for Microsoft Exchange 29
Managed PKI Installation Requirements 29
Local Hosting Server Requirements 29
Exchange Server Requirements 29
Go Secure! for Nortel 32
Managed PKI Installation Requirements 32
Additional Installation Requirements 32
CAPI-Enabled Nortel Implementation 33
Non-CAPI Enabled Nortel Implementation 33
Go Secure! for Web Applications 33
Managed PKI Installation Requirements 33
Application Server Requirements 34
For Hosting Windows 2000 or 2003 MSI Packages 35
End User Client Requirements 35

Chapter 4 Luna Token Reader Compatibility 37

Token Readers 37
Tokens 37

Index 39

CHAPTER 1

Introduction

Authentication Services Hardware/Software Requirements describes what your organization needs to set up VeriSign enterprise services from BT.

About this Manual

Authentication Services Hardware/Software Requirements is designed for BT's VeriSign Managed PKI Services customers and installers who need to know what equipment to buy for their enterprise configurations. This document contains lists of the hardware and software you must have to install these programs. For details about how to configure and set up VeriSign products, refer to the installation guides that accompany the respective products.

Note Read the appropriate hardware/software section for the product you want to install.

It is not possible for BT or VeriSign to test every combination of third-party client, server, operating system, service pack, and so on. However, BT and VeriSign do test the most common combinations and then, relying on the assertions of the vendors of these products, expands the list of supported combinations which are expected to work. For example, if a vendor asserts that a version of a Web browser is compatible with all versions of an operating system, BT or VeriSign tests products and services against the Web browser on the most common version of the operating system and relies on the vendor's statement to assume the Web browser works with all versions of the operating system.

If a problem arises with a combination which could not have been anticipated, BT and VeriSign are committed to assisting you to work around the issue. If BT or VeriSign cannot help you and cannot influence a timely patch to the 3rd party

product by the vendor, we will add it to a list of unsupported combinations which will be available in our knowledge base and in this document.

Note Regardless of the listings within this guide, BT Trust Services will support only CURRENT software versions from manufacturers. Any hardware or software products, which their manufacturers declare unsupported during the lifetime of this document, will also be unsupported by BT Trust Services.

This document is divided into the following sections:

- Chapter 2, "Managed PKI Requirements," lists the requirements for:

  "Managed PKI Administrator Workstation" on page 9

  "End User Machine" on page 10

  "Local Hosting" on page 10

  "Automated Administration Module" on page 12

  "Key Management Service" on page 14

  "Roaming" on page 16

  "Digital Notarization" on page 21

  "Certificate Validation Module (CVM)" on page 21

  "Certificate Parsing Module (CPM)" on page 23

  "Online Certificate Status Protocol (OCSP)" on page 24

- Chapter 3, "Go Secure! Requirements," lists the requirements for:

  "Go Secure! for Check Point" on page 25

  "Go Secure! for Lotus Notes" on page 27

  "Go Secure! for Microsoft Exchange" on page 29

  "Go Secure! for Nortel" on page 32

  "Go Secure! for Web Applications" on page 33

- Chapter 4, "Luna Token Reader Compatibility," lists the Luna token hardware requirements for Managed PKI.

Related Managed PKI Documents

Customer documentation for the VeriSign products described in this document are available on the various product CDs or from the Control Center *Download* page. If you did not receive product documentation or would like to order more copies of product documentation, contact your BT account manager for information.

Compatibility Matrix for Single Digital ID

The Compatibility Matrix shows which different VeriSign enterprise services, software, and hardware can be used with the same Digital ID.

Figure 1-1 Abbreviations used in the Compatibility Matrix

TstDrv	Test Drive	GS! LN	Go Secure! for Lotus Notes
KMS	Key Management Service	OCSP	Online Certificate Status Protocol
AA	Automated Administration	Roam	Roaming Service
PTA	Personal Trust Agent in Go Secure! for Web Applications	CVM	Certificate Validation Module
GS! MSE	Go Secure! for Microsoft Exchange	CPM	Certificate Parsing Module
Public CA	Public hierarchy	File Enc	File Encryption feature of Go Secure! for Web Applications
Priv CA	Private hierarchy	Publ Cy CA	Public ceremony
GS! Nrtl	Go Secure! for Nortel	DMS	Device Manufacturing Service
MPKI SSL	Managed PKI for SSL	BAS	Business Authentication Service
GS! CP	Go Secure! for Checkpoint	OA	Outsourced Authentication
XKMS	XML Key Management Specification	CAS	Consumer Authentication Service
PTS	Personal Trust Service in Go Secure! for Web Applications	Win2k Int	Windows 2000/XP integration with smart cards
MS EFS	Microsoft Encryption File Service Integration	Roam/CAPI	Roaming support for Cryptographic API
Trust Gate	Trust Gateway		

Find out if the products or services are compatible by looking at the intersection of the two items you are interested in. For example, if you want to check the features PTA (**A**), Automated Administration (**B**), and Local Hosting (**C**) (**ABC**), check if AB (PTA row and Automated Administration column) is compatible (the result is **Yes)**. Next, check if **AC** is compatible (**Yes**), and finally compare **BC (Yes)**. A **Yes**

indicates the two features compared work together and that a single Digital ID can be used for both the features to work. A **No** indicates incompatibility or these features are not designed to work together. A **Req'd** indicates the product requires Automated Administration and Local Hosting.

Note The following numbered notes corresponds to the numeric codes in the table.

1 Managed PKI for SSL and Managed PKI for SSL Premium Edition can only be issued under Public
2 TestDrive only issued under Public CA
3 IPSec issued under Private or shared (co-branded) CAs
4 Key Management Service incorporates Automated Administration functionality. So a separate Automated Administration server is not needed
5 TestDrive does not work with anything that requires Managed PKI CD or other downloads
6 Works with client certificates only
7 Passcode, Manual Authentication, and Automated Authentication, including KMS, are mutually exclusive
8 There is no site kit for IPSec or Managed PKI for SSL
9 Passcode can be made to work with Automated Administration using customization
10 CVM works with OCSP (CVM and OCSP are orthogonal).
11 Go Secure! for Check Point does not work with Key Management Service dual key certificates
12 Requires Automated Administration, which requires Local Hosting. For Go Secure! for Microsoft Exchange, Automated Administration and Local Hosting are required only if you are using Windows authentication, but optional otherwise
13 Roaming requires PTA in VeriSign crypto mode (does not work with TPM functionality)
14 PTA supports smart cards with the CAPI certificate store only
15 Code not used
16 File Encryption Feature requires PTA 2.x
17 XKMS does not work with manual authentication
18 Real-time XKMS validation requires OCSP Premium account. OCSP can validate certificates registered through XKMS
19 CPM and CVM work with native SSL client authentication. PTA 6.0 has added support for native SSL client authentication. PTS does not have support for native SSL client authentication
20 Key Management Service and Automated Administration require Local Hosting. Automated Administration and Local Hosting do not require Key Management Service
21 PTA and PTS profiles are interoperable in roaming mode
22 PTS requires Roaming
23 Microsoft does not currently support EFS certificates on smart cards. To use EFS, the certificate must be on the local hard drive. You can use the same certificates for Win2k logon (on a smart card) and for EFS (copy stored locally)
24 Smart card CSP required for Win2k logon. Microsoft Base CSP required for EFS. PTA works in CAPI mode only (PTA cannot use Verisign Certificate Store)
25 Java PTA currently only supports Roaming 1.x. It does not support Roaming 6.0. ActiveX PTA with TPM functionality does not support Roaming
26 Not supported by Java PTA. Supported by ActiveX PTA without TPM functionality
27 Not supported by Java PTA. Supported by ActiveX PTA, with or without TPM functionality

	Test Drive	KMS	AA	Local Host	PTA	GS! MSE	Public CA	Priv CA	Publ CyCA	IPSec	MPKI SSL	Pass code	GS! CP	GS! LN	OCSP	Roam	CVM, CPM	File Enc	GS! Ntl	DMS	Smart-cards	BAS	OA	Client VPN	XKMS	Access360	CAS	PTS	Win2k Int.	MS EFS	Roam /CAPI	Trust Gate
KMS	no (5)																															
AA	no (5)	no (4)																														
Local Host	no (5)	reqtd (20)	reqtd (20)																													
PTA	yes (28)	yes (27)	yes	yes																												
GS! MSE	no	yes	yes (12)	yes (12)	yes (27)																											
Public CA	yes (2)	yes	yes	yes	yes	yes																										
Priv CA	no (2)	yes	yes	yes	yes	yes	no																									
Cy CA	no	yes	yes	yes	yes	yes	no	no (1)																								
IPSec	yes	no (6)	no	no (8)	yes (6)	no (6)	no (3)	yes (3)	yes (3)																							
MPKI SSL	no	no (6)	no	no (8)	no (6)	no (6)	yes (1)	no (1)	no	no																						
Pass-code	yes	no (7)	no (9)	yes	yes	yes (9)	yes	yes	yes	no (6)	no (6)																					
GS! CP	yes	yes (11)	yes	yes	yes (27)	yes	no	yes	yes	no	no	yes																				
GS! LN	no (5)	yes	reqtd (12)	reqtd (12)	no	no	yes	yes	yes	no	no	no	no																			
OCSP	no (5)	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	yes	yes	no																		
Roam	no (5)	yes	yes	yes	yes (13,25)	no	yes	yes	yes	no (6)	no (6)	yes	no (6)	no	yes																	
CVM, CPM	no (5)	yes	yes	yes	yes (19)	yes	yes	yes	yes	no (6)	no (6)	yes	no (6)	no	yes (10)	no																
File Enc	no	yes	yes	yes	yes (16,26)	yes	yes	yes	yes	no (6)	no (6)	yes	no (6)	no	no	yes	no															
GS! Ntl	no	no	no	no (8)	yes (27)	no	no	yes	yes	yes	no	yes	no	no	yes	no	no	no														
DMS	no	no	no	no	no	no	yes	yes	yes	no	no	no	no	no	no	no	no	no	no													
Smart-cards	yes	yes	yes	yes	yes (14,26)	yes	yes	yes	yes	no	no	yes	no	no	yes	no	yes	no	no	no												
BAS	no	no	no	yes	yes	no	no	yes	yes	no	no	no	no	no	yes	yes	yes	no	no	no	yes											
OA	no	no (15)	reqtd (12)	reqtd (12)	yes	no	yes	yes	yes	no	no	no	no	no	yes	yes	yes	no	no	no	yes	no										
Client VPN	yes	yes	yes	yes	yes (27)	no	no	yes	no	yes	no	yes	yes	no	yes	no (17)	no	no	yes	no	no	no	no									
XKMS	no	no	yes (17)	no	no	no	yes	yes	yes	no	no	yes	no	no	yes (18)	no	no	no	no (6)	no	no	yes	yes	no								
Access360	no	no	no	no	no	no	no	no (1)	no	no	no	no	no	no	no	no	no	no	no (6)	no	no	no	no	no	no							
CAS	no	no	no	yes	no	no	yes	yes	yes	no	no	no	no	no	yes	no	no	no	no (6)	no	no	no	no	no	no	no						
PTS	no	no	yes	yes	yes (21)	no	yes	yes	yes	no (6)	no (6)	yes	no	no	yes	reqtd (22)	no (19)	no	no (6)	no	no	no	no	no	yes	no	no					
Win2k Int.	no	yes	reqtd (12)	reqtd (12)	yes (26)	yes	no	yes	yes	no	no	no (9)	yes	no	yes	no (24)	yes	no	yes	no	yes	no	no	no (15)	no	no	no	no				
MS EFS	no	yes	yes	yes	yes (26)	yes	no	yes	yes	no	no	no (9)	yes	no	yes	no (24)	yes	no	yes	no	yes (23)	no	no	no (15)	no	no	no	no	yes			
Roam /CAPI	no	yes	yes	yes	yes (26)	yes	yes	yes	yes	no	no	yes	yes	no	yes	yes	yes	no	yes	no	no	no	no	yes	no	no	no	yes	no	no		
Trust Gate	yes	no	no	no	no	no	no	yes	no	no	no	yes	no	no	yes	no	no	no	no	no	no	no	no	no	yes	no	no	no	no	no	no	

CHAPTER 2

Managed PKI Requirements

This document describes the hardware and software that have been tested for use with Managed PKI. You may find that earlier versions of hardware and/or software and service packs work well with Managed PKI and its options. However, the versions in this document are the ones that are supported by BT and VeriSign.

For the most current information about any Managed PKI version, refer to the Release Notes for that product.

Protocols and Ports

The numbers in the following list indicate **port numbers**.

End user → Local Hosting server: 443, https

Local Hosting server → Automated Administration/Key Manager server: 2003, TCP/IP

Automated Administration or Key Manager server → Data sources:

LDAP directory: 389, LDAP

Secure LDAP: 636, LDAP with SSL

Database: ODBC

Local Hosting (with Automated Administration or with Key Management Service 3.0) → BT Trust Services: 80, http

Figure 2-2 shows a common hardware configuration for a Managed PKI installation with Local Hosting, Go Secure! for Web Applications, and Key Management Service with built-in Automated Administration functionality.

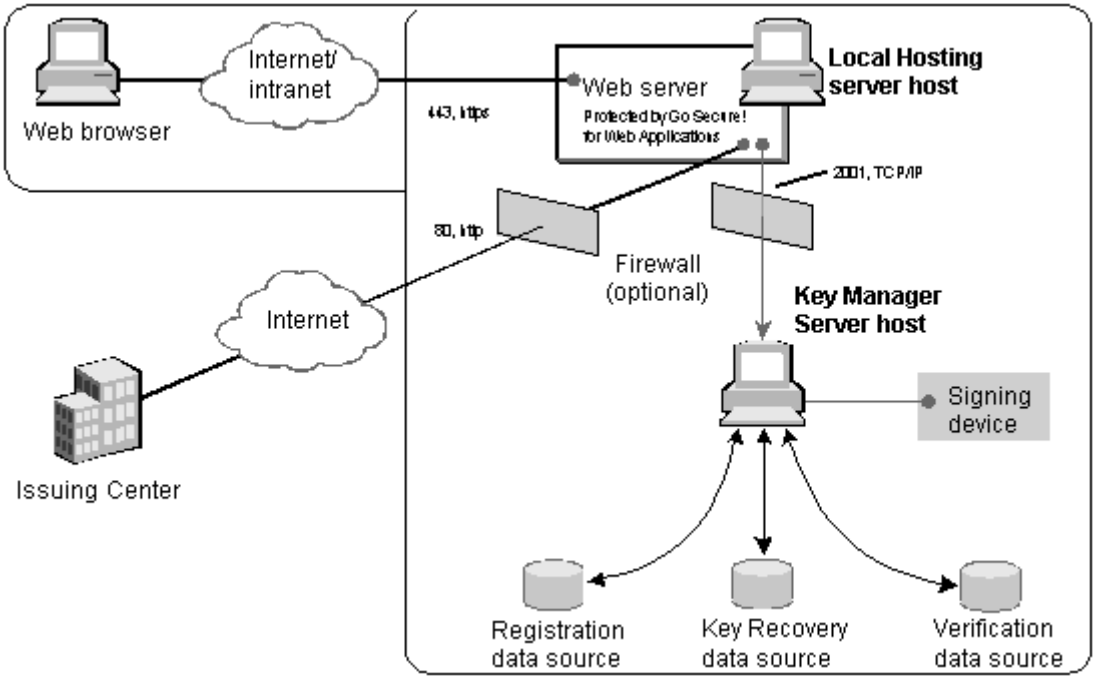

Figure 2-2 Typical configuration for Managed PKI with Key Management Service

Internet Access for Authentication Methods

There are three types of authentication methods that use Local Hosting:

- **Manual Authentication** (Local Hosting not required). Client/end user needs Internet access to BT Trust Services for this to work. Local Hosting can be used.
- **Passcode Authentication** (Local Hosting not required). Client/end user needs Internet access to BT Trust Services for this to work. Local Hosting can be used.
- **Automated Administration** (Local Hosting required). Client/end user does not need Internet access for this to work. The Local Hosting server needs access to the Authentication server and the Internet. A CGI on the Local Hosting server handles communication with BT Trust Services.

Managed PKI Administrator Workstation

This section describes hardware and software needed for the administrator's machine for Managed PKI and IPSec Managed PKI accounts.

Hardware

- Intel-based PC, 866Mhz Pentium or faster

> **Note** Lighter configurations will work but may not meet expected performance levels. In addition, adding more memory or a faster CPU to this configuration would probably not make a difference in performance. The administrator workstation must be able to access the Internet through port 443.

- 512MB RAM
- 10MB free disk space

Required for USB Token Users

- CD-ROM drive
- Aladdin token(s) and connector cable
- One available USB port for connecting the token

Supported Operating Systems

- Windows 2000 Service Pack 2 Professional (Restricted User Account)
- Windows 2003 Professional
- Windows ME
- Windows XP (Restricted User Account)

Supported Browsers

Browser capable of 128-bit crypto, with ActiveX and JavaScript support enabled.

- Netscape Communicator 4.75 or 8.0
- Internet Explorer 5.5, 6.0

End User Machine

CAUTION VeriSign has not tested and does not support Solaris, HP-UX, and Mac OS on the end user machine, although it may be assumed that Netscape 4.7 or 8.0 works on UNIX end user machines.

Operating System

- Windows 2000 Service Pack 2 Professional (Restricted User Account)
- Windows 2003 Professional
- Windows ME
- Windows XP (Restricted User Account)

Supported Browsers

Browser with 128-bit crypto, ActiveX and Javascript enabled

- Netscape Communicator 4.75 or 8.0
- Internet Explorer 5.5, 6.0

Note The end user machine must be able to access the Local Hosting server through port 443 and the Internet through port 443 if Automated Administration is not being used.

Local Hosting

To provide SSL-enabled access to your locally-hosted enrollment pages, you should install an appropriate server certificate. Although SSL is not required, it is highly recommended.

If used with Automated Administration or Key Management Service. Front-end Local Hosting server must be able to send outbound http on port 80 without being prompted for a proxy user ID or password. Also, if Local Hosting is on the same machine as Automated Administration, then Automated Administration only requires a Web server.

If used without Automated Administration and Key Management Service. The Local Hosting server does not need outbound access, but the end user does (on port 443).

Supported Web Server Applications

- Sun ONE Web Server 6.0 Service Pack 5
- Microsoft IIS 5.0 or 6.0
- Red Hat Stronghold (Apache) 4.0

Supported Local Hosting Web Server Operating Systems

- Solaris 8 or 9 (32-bit):
  - Sparc Ultra 2 or faster
  - 150MB free disk space
  - 512MB RAM
  - CD-ROM drive
- Windows 2000 Service Pack 2 or 2003:
  - Pentium, 866Mhz or faster
  - 100MB free disk space
  - 512MB RAM
  - CD-ROM drive
- Hewlett-Packard HP-UX 11i
  - B class workstation
  - 150MB free disk space
  - 512MB RAM
  - CD-ROM drive
- AIX 5.1:
  - 150MB free disk space

- 512MB RAM
- CD-ROM drive

Automated Administration Module

Requirements

- Automated Administration server: Automated Administration host with same requirements as Local Hosting server host, described below. (Can be on the same machine as Local Hosting server, although it is recommended that it be installed on a separate machine separated by a firewall.)
- Local Hosting module
- LDAP/ODBC database for validating shared secret data and/or registration of user certificates. Can be two separate databases or one.
- For the hardware token reader, the interface slot is a PCI slot. See Chapter 4, “Luna Token Reader Compatibility” for the specific token reader that applies.

Supported Local Hosting Web Servers

The front-end Local Hosting server used with Automated Administration must be able to send outbound http on port 80 without being prompted for a proxy user ID or password. For the requirements for shared Local Hosting/Automated Administration Web servers see “Local Hosting” on page 10.

Automated Administration Server

Note Most customers are able to edit the configuration file for the Automated Administration server to allow it to work with verification and registration data sources, and will therefore not need a compiler to customize the Automated Administration code.

Table 2-1 Platform configurations for AA servers

Operating Systems	Requirements	Optional (Compilers)
Windows 2000 Server Service Pack 2 or 2003	▪ Pentium, 866Mhz or faster ▪ 100MB free disk space ▪ 512MB RAM ▪ CD-ROM drive	*Optional, only if you want to customize:* Microsoft Visual C++ 6.0
Solaris 8 or 9 (32-bit)	▪ Sparc Ultra 5 or faster ▪ 150MB free disk space ▪ 512MB RAM ▪ CD-ROM drive	*Optional, only if you want to customize:* Sun Forte C/C++ Workshop 6.2, Update 2
Hewlett-Packard HP-UX 11i	▪ B class workstation ▪ 150MB free disk space ▪ 512MB RAM ▪ CD-ROM drive	*Optional, only if you want to customize:* HP package B.11.00_32/64, which includes a C++ B3911DB C.03.30
AIX 5.1	▪ 150MB free disk space ▪ 512MB RAM ▪ CD-ROM drive	*Optional, only if you want to customize:* VisualAge C++ Professional / C for AIX Compiler, Version 5.0

Automated Administration Data Sources

LDAP Directory

Automated Administration supports the following LDAP directories:

- Sun ONE Directory Server 5.1 SP1
- Lotus Domino 5.0.3, 6.0
- Windows 2000 Active Directory

- Windows 2003 Active Directory
- IBM SecureWay LDAP

ODBC

- Oracle 9i
- Microsoft SQL Server 7.0
- Microsoft SQL Server 2000
- Microsoft Access 2000

Key Management Service

Key Management Service requires Managed PKI, a Key Manager server with administrator privileges, and Local Hosting.

Requirements

- Key Manager server: Key Manager host with same requirements as Local Hosting server host, described below. (Can be on the same machine as Local Hosting server, although it is recommended that it be installed on a separate machine separated by a firewall.)
- Local Hosting module
- LDAP/ODBC database for validating shared secret data and/or registration of user certificates. Can be two separate databases or one.
- For the hardware token reader, the interface slot is a PCI slot. See Chapter 4, “Luna Token Reader Compatibility” for the specific token reader that applies.

Key Manager Server

It is recommended that the Key Manager server be a separate machine from Local Hosting, separated by a firewall.

Note Most customers are able to edit the configuration file for the Key Manager server to allow it to work with verification and registration data sources, and will therefore not need a compiler to customize the ODBC or LDAP code.

Table 2-2 Platform configurations for Key Manager servers

Operating Systems	Requirements	Optional (Compilers)
Windows 2000 Server Service Pack 2 or 2003	▪ Pentium, 866Mhz or faster ▪ 100MB free disk space ▪ 512MB RAM ▪ CD-ROM drive	*Optional, only if you want to customize:* Microsoft Visual C++ 6.0
Solaris 8 or 9 (32-bit)	▪ Sparc Ultra 5 or faster ▪ 150MB free disk space ▪ 512MB RAM ▪ CD-ROM drive	*Optional, only if you want to customize:* Sun Forte C/C++ Workshop 6.2, Update 2
Hewlett-Packard HP-UX 11i	▪ B class workstation ▪ 150MB free disk space ▪ 512MB RAM ▪ CD-ROM drive	*Optional, only if you want to customize:* HP package B.11.00_32/64, which includes a C++ B3911DB C.03.30
AIX 5.1	▪ 150MB free disk space ▪ 512MB RAM ▪ CD-ROM drive	*Optional, only if you want to customize:* VisualAge C++ Professional / C for AIX Compiler, Version 5.0

Local Hosting Server

The front-end Local Hosting server used with Key Management Service must be able to send traffic though outbound ports 80 and 443 without being prompted for a proxy user ID or password. For configuration information, see “Local Hosting” on page 10.

Key Manager Data Sources

The Key Manager data sources include the following:

- Verification
- Registration
- Key Recovery (each escrowed key requires approximately 6k of disk space)

Data sources should be replicated for redundancy, high availability, and fail-over.

LDAP Directory

Key Management Service supports the following LDAP directories:

- Sun ONE Directory Server 5.1 SP1 (SSL cannot be used between the Key Manager server and an SunONE LDAP server on HP-UX.)
- Lotus Domino 5.0.3. 6.0
- Windows 2000 Active Directory
- Windows 2003 Active Directory
- IBM SecureWay LDAP 3.2.2

ODBC

Key Management Service supports the following ODBC directories:

- Oracle 8i, 9i
- Microsoft SQL Server 7.0

Roaming

Two versions of Roaming are available:

- Roaming Service–All of the servers are hosted at the customer site.
- Enterprise Roaming–Some or all of the servers are hosted at BT's secure facility.

Roaming Service

This section describes the hardware and software requirements for customers implementing VeriSign's Roaming Service.

In this configuration, the customer hosts all servers. Servers should be replicated for redundancy, high availability, and fail-over.

VeriSign software required to run the Roaming service:

- Roaming and Storage back-end Server package
- Roaming Service Center Web Server package
- Roaming/Storage front-end Web server package

- Roaming/Storage Database package

Roaming Service Center Administrator Workstation(s)

Must be a separate machine from the Managed PKI Administrator workstation machine. Two or more machines should act as the Roaming Service Center administrator workstation, although they do not need to be dedicated. If administrator certificates are stored in the browser, different administrator certificates should be stored in browsers on different machines.

Administrator requirements are the same as for the Managed PKI Administrator requirements described on page 9.

Roaming and Storage Back-End Servers

Each back-end server and its hot spare must access the same database, so that the spare has access to the same state as the live server. This machine must be on the customer's production network, to have access to the Roaming and Storage Database machine. It should also be behind a firewall.

Table 2-3 Roaming and Storage back-end servers

Operating Systems	Requirements	Web Server(s) supported
Solaris 2.6 Patch 105591-09 installed. The patch is available at **http://access1.sun.com/**	▪ Sparc Ultra 10 or faster ▪ 9 GB free disk space ▪ 256MB RAM ▪ CD-ROM drive ▪ Perl 5.6.0 ▪ Oracle Client software	▪ Sun ONE (formerly iPlanet Enterprise Edition) Web server 4.0, 6.0 ▪ Secure Server ID installed in Web server (*required*)
Solaris 7 or 8	▪ Sparc Ultra 10 or faster ▪ 9 GB free disk space ▪ 256MB RAM ▪ CD-ROM drive ▪ Perl 5.6.0 ▪ Oracle client software	▪ Sun ONE (formerly iPlanet Enterprise Edition) Web server 4.0, 6.0 ▪ Secure Server ID installed in Web server (*required*)

Roaming and Storage Front-End Servers

The Roaming and Storage front-end servers can be run on existing Web Server machines.

There should be two Roaming and Storage front-end servers, each one communicating through a firewall with one Roaming and Storage back-end server. These machines do not need to be dedicated to the Roaming and Storage front-end server functionality. Front-end server plug-in can send outbound TCP to the Roaming and Storage back-end server

Table 2-4 Roaming and Storage front-end servers

Operating Systems	Requirements	Web Server(s) supported
Solaris 8	▪ Sparc Ultra 10 or faster ▪ 9 GB free disk space ▪ 256MB RAM ▪ CD-ROM drive ▪ Perl 5.6.0	▪ Sun ONE (formerly iPlanet Enterprise Edition) Web server 4.0, 6.0 ▪ Secure Server ID installed in Web server (*optional*)

Roaming and Storage LDAP Database

The Roaming and Storage LDAP database must have read/write access to the back-end Roaming and Storage server, but must be installed on a separate machine. This database should be replicated for redundancy, high availability, and fail-over.

The Roaming and Storage LDAP database supports Sun ONE Directory Server 5.1 with Service Pack 1.

Enterprise Roaming

Enterprise Roaming comes in two options, depending on where the roaming servers are installed: Outsourced Roaming or Split Hosting.

- With Outsourced Roaming, all Roaming servers are installed and operated in BT's secure facility.
- With Split Hosting, some of the Roaming servers are installed and operated in BT's secure facility, and the rest are installed and operated by the enterprise.

Outsourced Roaming

Outsourced Roaming does not require the customer to host any machines other than the administrator workstation. The requirements are the same as for the Managed PKI Administrator requirements described on page 9.

Split Hosting

This section describes the hardware and software requirements for customers implementing Split Host Roaming.

In this configuration, the customer hosts all servers. Servers should be replicated for redundancy, high availability, and fail-over.

VeriSign software required to run Split Hosting:

- Roaming and Storage Back End Server package
- Roaming Service Center Web Server package
- Roaming/Storage front end Web server package
- Roaming/Storage Database package

Roaming Service Center Administrator Workstation(s)

Must be a separate machine from the Managed PKI Administrator workstation machine. Two or more machines should act as the Roaming Service Center administrator workstation, although they do not need to be dedicated. If administrator certificates are stored in the browser, different administrator certificates should be stored in browsers on different machines.

Administrator requirements are the same as for the Managed PKI Administrator requirements described on page 9.

Roaming and Storage Back-End Servers

Each back-end server and its hot spare must share the same database, so that the spare has access to the same state as the live server. This machine must be on the customer's production network, to have access to the Roaming and Storage Database machine. It should also be behind a firewall.

Table 2-5 Roaming and Storage back-end servers

Operating Systems	Requirements	Web Server(s) supported
Solaris 2.6 Patch 105591-09 installed. The patch is available at **http://access1.sun.com/**	▪ Sparc Ultra 10 or faster ▪ 9 GB free disk space ▪ 256MB RAM ▪ CD-ROM drive ▪ Perl 5.6.0 ▪ Oracle Client software	▪ Sun ONE (formerly iPlanet Enterprise Edition) Web server 4.0, 6.0 ▪ Secure Server ID installed in Web server (*required*)
Solaris 7 or 8	▪ Sparc Ultra 10 or faster ▪ 9 GB free disk space ▪ 256MB RAM ▪ CD-ROM drive ▪ Perl 5.6.0 ▪ Oracle client software	▪ Sun ONE (formerly iPlanet Enterprise Edition) Web server 4.0, 6.0 ▪ Secure Server ID installed in Web server (*required*)

Roaming and Storage Front-End Servers

The Roaming and Storage front-end servers can be run on existing Web Server machines.

There should be two Roaming and Storage front-end servers, each one communicating through a firewall with one Roaming and Storage back-end server. These machines do not need to be dedicated to the Roaming and Storage front-end server functionality. Front-end server plug-in can send outbound TCP to the Roaming and Storage back-end server

Table 2-6 Roaming and Storage front-end servers

Operating Systems	Requirements	Web Server(s) supported
Solaris 8	▪ Sparc Ultra 10 or faster ▪ 9 GB free disk space ▪ 256MB RAM ▪ CD-ROM drive ▪ Perl 5.6.0	▪ Sun ONE (formerly iPlanet Enterprise Edition) Web server 4.0, 6.0 ▪ Secure Server ID installed in Web server (*optional*)

Roaming and Storage LDAP Database

The Roaming and Storage LDAP database must have read/write access to the back-end Roaming and Storage server, but must be installed on a separate machine. This database should be replicated for redundancy, high availability, and fail-over.

The Roaming and Storage LDAP database supports Sun ONE Directory Server 5.1 with Service Pack 1.

Roaming Back End Server

These machines have the same requirements as the Roaming and Storage Back End Servers on page 19.

Roaming Front End Servers

These machines have the same requirements as Roaming and Storage Front End Servers on page 20.

Roaming Database

The Roaming Database is a separate instance of an Oracle database, apart from the Roaming and Storage database. This instance is used by the Roaming Server and its hot spare. This does not require an additional machine; rather, it requires a separate database instance which can reside on the Roaming and Storage Database machine. The requirements are the same as Roaming and Storage Database on page 21.

Digital Notarization

Digital Notarization is a VeriSign back-end service that is accessed from the Managed PKI Control Center. This requires no installation at the customer site.

Web Browser Requirements

- Netscape Communicator 4.5, 4.7 or 8.0
- Internet Explorer 5.5, 6.0

Certificate Validation Module (CVM)

The CVM plug-in should be installed on the Web server. To access the Certificate Validation Module from the Web, use any Web browser that supports SSL client authentication.

Platforms Supported

CVM is supported on the following platforms:

- Windows 2000 Service Pack 2 or Windows Server 2003:
  - Pentium, 866Mhz or faster
  - 10MB free disk space
  - 128MB RAM
  - CD-ROM drive
- Solaris 8 or 9:
  - Sparc Ultra 2 or faster
  - 10MB free disk space
  - 128MB RAM
  - CD-ROM drive
- HP-UX 11i:
  - 10MB free disk space
  - 128MB RAM
  - CD-ROM drive

CVM Web Server Plug-In

- Microsoft IIS 5.0, 6.0
- SunONE Web Server 6.0, Service Pack 5
- Red Hat Stronghold (Apache) 3.0, 4.0 (not supported on Windows platforms)

Certificate Parsing Module (CPM)

VeriSign provides two CPM implementations:

- Server plug-in version (NSAPI or SAF). The server plug-in can be used with any other server plug-ins and extensions such as servers, javascript, CGI programs in any programming language (csh, Perl, C, C++), NSAPI modules, and so on.
- Toolkit

Both support SunONE Web Server 6.0, Service Pack 5 on the following operating systems:

- Windows 2000:
  - Pentium, 866Mhz or faster
  - 10MB free disk space
  - 128MB RAM
  - CD-ROM drive
- Solaris 8 or 9:
  - Sparc Ultra 2 or faster
  - 10MB free disk space
  - 128MB RAM
  - CD-ROM drive
- Hewlett-Packard HP-UX 11i or AIX 5.1
  - 10MB free disk space
  - 128MB RAM
  - CD-ROM drive

Server Plug-in

CPM is available as a server plug-in for SunONE Web Server 6.0.

VeriSign provides example CGI programs that use the server plug-in for:

- C and C++ for Bourne shell and C shell
- Perl for Bourne shell and C shell.

Online Certificate Status Protocol (OCSP)

Online Certificate Status Protocol (OCSP) requires no installation at the customer site besides the CVM plug-in, which can be modified to access OCSP.

Browser Requirements

Any Web browser that supports SSL client authentication.

CHAPTER 3

Go Secure! Requirements

Go Secure! for Check Point

Managed PKI Installation Requirements

Table 3-7 shows the Managed PKI requirements for Go Secure! for Check Point.

Table 3-7 Managed PKI options used with Go Secure! for Check Point

CD	Local Hosting	Authentication Methods	Key Management Service	Other
Required: ▪ Managed PKI Local Hosting CD ▪ Go Secure! for Checkpoint CD ▪ Managed PKI AA CD (optional)	Optional	▪ Manual Authentication ▪ Automated Administration ▪ Passcode Authentication	Optional	IPSec Private Managed PKI administrator certificate

Browser

Browser capable of 128-bit crypto, with JavaScript support enabled.

- Netscape Communicator 4.75 or 8.0
- Internet Explorer 5.5, 6.0

SecuRemote Version

- SecuRemote 4.1 SP2, Build number 4.1.6.5

- SecuRemote NG FP3, Build number 53328

VPN-1 Gateway

Hardware and software requirements for your VPN-1 gateway vary based on the solution you implement. For guidance on the VPN-1 gateway solution you should implement, refer to Check Point.

SecuRemote and SecureClient Workstation

Hardware and software requirements for your SecuRemote and SecureClient workstation vary based on the solution you implement. For guidance on the SecuRemote and SecureClient workstation solution you should implement, refer to Check Point.

Directory Object Module (DOM) Requirements

If you implemented an access control list (ACL) with SecuRemote 4.1, DOM is required to automatically populate your ACL. SecuRemote NG does not require an ACL to authorize user access.

DOM runs on the following platforms:

- Windows
- Solaris
- Nokia with IPSO

Note HP-UX and AIX do not support the VeriSign DOM. Users of a VPN-1 gateway on HP-UX or AIX can perform DOM functions from a Solaris or Windows platform.

DOM Integration with LDAP

You need access to installation instructions for the following software:

- Netscape Directory Server 4.1x. Information is available at **www.sun.com** under **Products and Services → Web and Directory Servers**.
- Check Point Account Management Console (AMC). The Check Point v4.0 CD contains the AMC installation software.

Intel Platforms with Windows NT 4.0 SP4 or SP6a

Processor	RAM	Disk Space	Directory Server
866MHz	64 MB	100MB	Netscape Directory Server 4.11

Sun Platforms with Solaris 2.6

Processor	RAM	Disk Space	Directory Server
Sparc Ultra 2 or faster	64 MB	150MB	Netscape Directory Server 4.11
Solaris 8 (not tested)	64MB	150Mb	Netscape Directory Server 4.11

Go Secure! for Lotus Notes

Go Secure! for Lotus Notes requires at least two servers: the Web server and the Domino server. Go Secure! for Lotus Notes works in a configuration with single or multiple Domino servers. If you are also implementing the optional Key Management Service, refer to “Key Management Service” on page 14.

Managed PKI Installation Requirements

Table 3-8 shows the Managed PKI requirements for Go Secure! for Lotus Notes 6.0.

Table 3-8 Managed PKI options used with Go Secure! for Lotus Notes

CD	Local Hosting	Authentication Methods	Key Management Service
Required: ▪ Managed PKI Local Hosting CD ▪ Go Secure! for Lotus Notes CD ▪ Managed PKI AA CD	Required	Automated Administration only	Optional. Supports both single key mode and dual key mode.

Local Hosting Web Server Operating Systems

- Windows 2000 or 2003

- Solaris 8 or 9
- AIX 5.1

Web Servers

- IIS 5.0 or 6.0
- Sun ONE Web server (formerly iPlanet Enterprise Edition) 4.1 or 6.0

Notes Client Requirements

Notes Client Version 5.02 or higher, or 6.0 or 6.01 on the following operating systems:

- Windows 2000
- Windows XP (Notes Client 6.0, 6.01 only)

Limitations and Assumptions in Go Secure! for Lotus Notes

The following assumptions and limitations apply to the current version of Go Secure! for Lotus Notes:

- The client authentication support is limited. Certificates issued by Go Secure! for Lotus Notes can be used to access a Lotus Domino server. However, the Certificate Validation Module is not available for the Domino server and instructions in the e-mail to the users are oriented towards use of certificates with S/MIME.
- Customizing the enrollment e-mail content requires a thorough knowledge of Lotus scripts.
- When the *Format preference for incoming mail* field in Person Document is set to *Prefers MIME*, the document links, URLs, and other Rich Text Format will be disabled in the outgoing email. This is a limitation in the Lotus Notes client application.

Hierarchical ID File Usage

For the LDAP Directory Integration to work, your organization should use hierarchical ID files. Lotus Notes R5/R6 servers and clients cannot create new flat ID files.

Go Secure! for Microsoft Exchange

Managed PKI Installation Requirements

Table 3-9 shows the Managed PKI requirements for Go Secure! for Microsoft Exchange.

Table 3-9 Managed PKI options used with Go Secure! for Microsoft Exchange

CD	Local Hosting	Authentication Methods	Key Management Service
Required: ▪ Managed PKI Local Hosting CD ▪ Go Secure! for Microsoft Exchange CD Optional: ▪ Managed PKI AA CD ▪ Go Secure! for Web Applications CD	Optional	▪ Manual Authentication ▪ Passcode Authentication ▪ Automated Administration ▪ Windows authentication (Requires the Automated Administration module)	Optional

Local Hosting Server Requirements

If you are hosting locally, you must install the Go Secure! for Microsoft Exchange site kit on the same server as your Local Hosting site kit. If you are also implementing the optional Key Management Service, refer to “Key Management Service” on page 14.

Supported Local Hosting Web Server Operating Systems

Windows 2000 or 2003

Supported Local Hosting Web Servers

IIS 5.0 or 6.0

Exchange Server Requirements

The Exchange server can be Windows 2000 or 2003 server.

Windows 2000 Server or 2003 Server

- Pentium, 866Mhz or faster
- 100MB free disk space
- 256MB RAM
- Microsoft Exchange Server 5.5 with Service Pack 3, or Microsoft Exchange Server 2000 or 2003
- Domain controller is Windows 2000 or 2003 with Active Directory, with either
  - No Active Directory Connector (ADC), *or*
  - Active Directory Connector replicating data between the Active Directory and Exchange directory.

CAUTION Microsoft Exchange Server and the Windows domain controller should be on separate machines.

Exchange Server 5.5

The Exchange Server schema must be such that the Mailbox object includes following LDAP attributes:

- cn
- alias
- rfc822Name
- userCertificate
- userSMIMECertificate

Exchange Server 2000 or 2003

The Exchange Server schema must be such that the User object on the Active Directory includes the following LDAP attributes:

- cn
- alias
- rfc822Name

- userCertificate
- userSMIMECertificate
- legacyExchangeDN
- directoryName

Directory Replication

If multiple Exchange Servers are involved then directory replication must be enabled in such a way that all of the above mentioned attributes are replicated. Each of the above mentioned LDAP attribute names have a different name as seen from the Exchange Administrator console. For example, the LDAP attribute userCertificate is referred as X509-Cert in Exchange Administrator console.

If Using a Mix of Exchange 5.5 Servers and Exchange 2000 or 2003 Servers

In this case, directory replication must be enabled using an Active Directory Connector (ADC). The ADC is installed on the respective Domain Controllers (which are also Active Directory Servers) and help in replicating information between the Exchange 5.5 directory and the Active Directory.

End User Mailboxes

All users who are going to enroll for a Go Secure! for Microsoft Exchange certificate must have a mailbox created on an Exchange Server. The mailbox must have a valid “Primary NT Account” value, as displayed in the mailbox property sheet through the Exchange Administrator Console.

End User Machine Requirements

- Internet Explorer 5.5, or 6.0
- Outlook 2000 or 2002
- MSI packages supplied on Go Secure! for Microsoft Exchange CD or on the *Download* page of the Control Center.

Go Secure! for Nortel

Managed PKI Installation Requirements

Table 3-10 shows the Managed PKI requirements for Go Secure! for Nortel.

Table 3-10 Managed PKI options used with Go Secure! for Nortel

CD	Local Hosting	Authentication Options	Key Management Service	Other
Managed PKI Local Hosting CD There is a Go Secure! for Nortel CD, which is documentation only and not required.	No	▪ Passcode Authentication (recommended) ▪ If you are **not** using Quickstart or Full Managed PKI, you will have to use Manual Authentication	No	IPSec Private Managed PKI administrator certificate

Additional Installation Requirements

- Verify that the client computer that you use to test the VPN implementation is set up as follows:
  - For extranet access over a dial-up connection:
    - Microsoft TCP/IP is installed.
    - A modem or other dial-up connection device is configured.
    - A PPP account is available through a corporate account or an Internet Service Provider (ISP).
    - Dial-Up Networking is installed. You can create a dial-up networking phone book entry to dial the ISP's point of presence (POP). Enter the information requested in Dial-Up Networking to enter the telephone number, User ID, and password supplied by the ISP.
  - For extranet access over a LAN connection:
    - TCP/IP is installed and running over a LAN adapter (NIC card).

– A working network connection is in place.

CAPI-Enabled Nortel Implementation

For a CAPI-enabled Nortel implementation, use:

- Nortel Client version 4.65.
- Nortel Contivity Extranet Switch and Server version that supports Nortel Client version 4.65. For information on Nortel switches and servers, contact Nortel Networks Customer Support.

Non-CAPI Enabled Nortel Implementation

For a non-CAPI enabled Nortel implementation, use:

- Nortel Client version 2.6 or higher.
- Nortel Contivity Extranet Switch and Server version that supports Nortel Client version 2.6. For information on Nortel switches and servers, contact Nortel Networks Customer Support.

Go Secure! for Web Applications

Managed PKI Installation Requirements

Table 3-11 shows the Managed PKI requirements for Go Secure! for Web Applications.

Table 3-11 Managed PKI options used with Go Secure! for Web Applications

CD	Local Hosting	Authentication Options	Key Management Service	Other
▪ Managed PKI Local Hosting CD ▪ Go Secure! for Web Applications CD ▪ Managed PKI AA CD (optional)	Optional	▪ Manual Authentication ▪ Passcode Authentication ▪ Automated Administration	Optional	Optional: ▪ Roaming ▪ PTS

Application Server Requirements

Supported Application Server Operating Systems

- Windows 2000
  - Pentium, 866Mhz or faster
  - 20MB free disk space
  - 128MB RAM
- Solaris 8 or 9
  - Sparc Ultra 2 or faster
  - 20MB free disk space
  - 128MB RAM
- Hewlett-Packard HP-UX 11i
  - 20MB free disk space
  - 128MB RAM
- AIX 5.1
  - 20MB free disk space
  - 128MB RAM

Supported Application Server Web Servers

- IIS 5.0
- SunONE Web Server 6.0
- Red Hat Stronghold (Apache) 3.0, 4.0

WebSphere and WebLogic Application Server Integration

The PTA application server integrates with the IBM WebSphere Application Server v3.5 and WebLogic server 6.0 and above. Supported hardware platforms and Web server software are shown in “Application Server Requirements” on page 34.

Note If you use the PTA for transaction signing and you want to customize the authentication server code, install the appropriate development environment as described on page 13.

Netegrity SiteMinder Integration

The PTA server implements a custom authentication scheme that integrates with Netegrity's SiteMinder 5.0. Supported software platforms are Solaris 8 or 9, or Windows 2000.

Signature Verification API Supported

Windows 2000 and Windows Server 2003 implement a COM version of Signature Verification API. This allows enterprises to verify digital signatures in the Microsoft ASP environment. This support includes the standard capabilities of the PTA server suite such as chain validation and revocation checking based on CRLs and OCSP.

For Hosting Windows 2000 or 2003 MSI Packages

- Windows 2000 or 2003 Domain Controller
- Active Directory to specify the Group policies.

For specific information, refer to Microsoft Technet at:

http://www.microsoft.com/technet

End User Client Requirements

ActiveX-based PTA

ActiveX-based PTA works only for browsers using Microsoft Windows operating systems.

Supported Operating Systems for ActiveX-based PTA

- Windows 2000
- Windows XP

Supported Browsers for ActiveX-based PTA

- Internet Explorer 5.5, 6.0 (domestic and international)
- Netscape Communicator 4.75 (domestic and international)

Java-based PTA

Java-based PTA is supported by the following operating systems and browsers:

Supported Operating Systems for Java-based PTA

- Linux 2.4
- Solaris 8
- Windows 2000
- Windows XP

Supported Browsers for Java-based PTA

End-user browsers must have Java plug-in 1.41.

- Internet Explorer 5.5, 6.0 (domestic and international)
- Netscape Communicator 8.0 (domestic and international)

PTS

PTS works on any browser with Internet access and JavaScript enabled.

CHAPTER 4

Luna Token Reader Compatibility

BT Trust Services ships token readers with Managed PKI for use with the Automated Administration and Key Management Service modules.

Token Readers

For Managed PKI, BT supports only the Chrysalis-ITS LunaDock reader, which is an external reader that requires a hardware PCI slot. The reader requires the following version of the driver. Older models of token readers are not supported, and earlier versions of the driver are not supported.

- For token readers on Windows, Solaris, or AIX platforms, use version 8.1
- For token readers on HP-UX platforms, use version 8.2

Tokens

For Managed PKI, BT supports only the Luna 2 token (firmware 3.9)

Note IBM Netfinity is incompatible with Luna token readers.

Index

A

Automated Administration **8**, **12**
- compatibility matrix **3**
- data sources **13**
- Go Secure! for Checkpoint with **25**
- Go Secure! for Lotus Notes **27**
- Go Secure! for Microsoft Exchange **29**
- Go Secure! for Web Applications **33**
- protocols and ports **7**
- requirements **12**
- server **13**

B

browsers
- Certificate Validation Module **21**
- Digital Notarization **21**
- Go Secure! for Checkpoint **25**
- Managed PKI administrator workstation **9**
- Managed PKI end user **10**
- Online Certificate Status Protocol **24**

Business Authentication Service
- compatibility matrix **3**

C

CAPI-enabled Nortel implementation **33**

Certificate Parsing Module **23**
- compatibility matrix **3**

Certificate Validation Module
- compatibility matrix **3**

Client Managed PKI
- *see* Managed PKI

compilers
- AIX **13**, **15**
- HP-UX **13**, **15**
- Solaris **13**, **15**
- Windows 2000 **13**, **15**

Consumer Authentication Service
- compatibility matrix **3**

CPM
- *see* Certificate Parsing Module

CVM
- *see* Certificate Validation Module

D

Device Manufacturing Service
- compatibility matrix **3**

Digital Notarization **21**

Directory Server **27**

documentation **3**

Domino servers **27**

E

end users
- Exchange server requirements for **31**
- Go Secure! for Web Applications client requirements **35**
- Managed PKI requirements for **10**
- protocols and ports **7**

Enterprise Roaming **18**

Exchange server **29**

F

File Encryption feature
- compatibility matrix **3**

G

Go Secure! for Checkpoint **25**
compatibility matrix **3**
Managed PKI requirements for **25**
Go Secure! for Lotus Notes
compatibility matrix **3**
Go Secure! for Lotus Notes R5
limitations and assumptions **28**
Managed PKI requirements for **27**
Go Secure! for Microsoft Exchange **29**
compatibility matrix **3**
Go Secure! for Nortel
additional installation requirements for **32**
CAPI-enabled Nortel implementation **33**
compatibility matrix **3**
Managed PKI requirements for **32**
non-CAPI enabled Nortel implementation **33**
Go Secure! for Web Applications **33**
Managed PKI requirements for **33**

I

ID file usage **28**
IPSec Managed PKI
Go Secure! for Checkpoint with **25**
Go Secure! for Nortel with **32**
IPSec Managed PKI administrator workstation **9**

K

Key Management Service **14**
compatibility matrix **3**
Go Secure! for Checkpoint with **25**
Go Secure! for Lotus Notes with **27**
Go Secure! for Microsoft Exchange with **29**
Go Secure! for Nortel with **32**
Key Manager server **14**
protocols and ports **7**

L

LDAP
see Lightweight Directory Access Protocol
Lightweight Directory Access Protocol
Automated Administration with **13**, **16**
Go Secure! for Checkpoint with **26**
Key Management Service with **16**
protocols and ports **7**
supported directories **13**, **16**
Local Hosting **11**
Automated Administration with **11**
Go Secure! for Checkpoint with **25**
Go Secure! for Lotus Notes with **27**
Go Secure! for Microsoft Exchange with **29**
Go Secure! for Web Applications with **33**
Key Management Service with **11**
protocols and ports **7**
Luna token **37**
Luna token reader **37**

M

Managed PKI administrator workstation **9**
Managed PKI for SSL
compatibility matrix **3**
Managed PKI requirements
administrator workstation **9**
Go Secure! for Checkpoint **25**
Go Secure! for Lotus Notes R5 **27**
Go Secure! for Microsoft Exchange **29**
Go Secure! for Nortel **32**
Go Secure! for Web Applications **33**
Manual Authentication **8**
Go Secure! for Checkpoint with **25**
Go Secure! for Microsoft Exchange with **29**
Go Secure! for Nortel **32**
Go Secure! for Web Applications **33**

manuals
see documentation
MSI package **35**

N

Netegrity SiteMinder **35**
non-CAPI enabled Nortel implementation **33**

O

ODBC
Automated Administration with **14**, **16**
protocols and ports **7**
Online Certificate Status Protocol **24**
compatibility matrix **3**
operating system
Automated Administration **13**
Go Secure! for Checkpoint with **26**
Key Management Service **15**
Managed PKI administrator workstation **9**
Managed PKI end user machine **10**
Roaming Service **18**, **20**
Outsourced Authentication
compatibility matrix **3**
Outsourced Roaming **18**

P

Passcode Authentication **8**
Go Secure! for Checkpoint with **25**
Go Secure! for Microsoft Exchange **29**
Go Secure! for Nortel **32**
Go Secure! for Web Applications **33**
Personal Trust Agent
compatibility matrix **3**
requirements for **33**
Personal Trust Service **36**
compatibility matrix **3**
Go Secure! for Web Applications **33**
protocols and ports **7**
PTA
see Personal Trust Agent
PTS
see Personal Trust Service

R

requirements
Automated Administration **12**
Certificate Parsing Module **23**
Digital Notarization **21**
Exchange server **29**
Go Secure! for Checkpoint **25**
Go Secure! for Microsoft Exchange **29**
Go Secure! for Web Applications **33**
Key Management Service **14**
Lightweight Directory Access Protocol **26**
local hosting **11**
Lotus Notes R5 **27**
Luna tokens and reader **37**
Managed PKI administrator workstation **9**
Managed PKI end user machine **10**
Notes Client **28**
Online Certificate Status Protocol **24**
Roaming service **16**, **19**
Web server **22**, **28**
roaming & storage front end servers
communicating with roaming & storage back end servers **20**
roaming and storage
back end servers **17**, **19**
back end servers communicating with roaming and storage front end servers **20**
front end servers **17**, **20**
Roaming and Storage LDAP database **18**, **21**
roaming database **21**

Roaming Service
compatibility matrix **3**
Go Secure! for Web Applications **33**
Outsourced configuration **18**
split hosting configuration **19**
Roaming service center **19**
administrator workstation **17**, **19**
roaming and storage back end servers **17**, **19**
roaming and storage front end servers **17**, **20**
Roaming database **21**
see also enterprise hosting

S

Secure Server ID **18**, **20**
SecureClient **26**
SecuRemote **25**, **26**
servers
see Web servers
Signature Verification API **35**

T

token reader
see Luna token reader
tokens
see Luna token
Trust Gateway
compatibility matrix **3**

V

VPN-1 Gateway **26**

W

Web servers
Automated Administration **12**
Certificate Validation Module **22**, **24**
Domino **27**
Go Secure! Lotus Notes **27**
Key Management Service **14**
Local Hosting **10**, **11**
WebLogic Application Server **34**
WebSphere Application Server **34**
Windows authentication
Go Secure! for Microsoft Exchange **29**

X

XKMS
see XML Key Management Specification
XML Key Management Specification
compatibility matrix **3**